DBCONCEPTS

DBCONCEPTS WHITEPAPER

8 GRÜNDE, WARUM ENDPOINT DETECTION UND RESPONSE (EDR) NICHT MEHR AUSREICHT

www.dbconcepts.com

Einleitung

Spektakuläre Hackerangriffe wie der, durch ein verseuchtes Update der SolarWinds-Software Orion, die Computersysteme Tausender US-Behörden und Unternehmen kompromittierte, sowie die exponentielle Zunahme von Ransomware-Angriffen auf der ganzen Welt haben dazu geführt, dass das Thema **Cybersicherheit** in den Vorstandsetagen aller Branchen zu einer Priorität geworden ist.

Trotz jahrelanger erheblicher Investitionen in Schulungen, Tools und Dienstleistungen im Bereich der Cybersicherheit gibt es keine Anzeichen dafür, dass die Zahl der Angriffe nachlässt. Lösungen wie Endpoint Detection and Response (EDR) sind zwar sehr vielversprechend, konnten aber nicht zur Reduktion von Ransomware-Angriffen beitragen; im Gegenteil, die Zahl der Angriffe und ihre Auswirkungen auf Unternehmen nehmen jedes Jahr erheblich zu.

Die Auswirkungen auf Unternehmen sind immens: Laut Data-Breach Report[1] erreichten 2022 die durchschnittlichen Data-Breach Kosten einen Rekordhoch von 4,38 Millionen USD - Tendenz steigend. In dem Bericht werden Kostenfaktoren, wie rechtliche, regulatorische und technische Aktivitäten, Image-, und Markenwertverlust, Kundenfluktuation und Beeinträchtigung von Mitarbeiterproduktivität berücksichtigt. 83 % der befragten Unternehmen waren von **mehr als einem** „Data Breach“ betroffen.

Menschliches Versagen ist nach wie vor eine der Hauptursachen für Sicherheitsverletzungen, da Phishing immer schwieriger zu erkennen ist und Fehlkonfigurationen und Alarmmüdigkeit die überlasteten SOC-Teams plagen. Zero-Day-Schwachstellen und das Fehlen konsequenter Patches, die eine weitere Ausnutzung der Angriffsvektoren verhindern, sorgen für zusätzliche Unruhe.

Zunahme Ransomware	Zunahme Cyberattacken	Identifikation & Eindämmung
ÜBER 800 %	77 %	287 TAGE
2021 Mid-Year Cyber Threat Landscape Report	EY Global Information Security Survey (GISS)	IBM Cost of Data Breach Report

1 https://www.ibm.com/reports/data-breach

Insider-Bedrohungen, ob absichtlich oder versehentlich, nehmen weiter zu, insbesondere angesichts von Remote-Arbeit und einer schwer zu kontrollierenden Software-Lieferkette. Forrester Research [1]prognostiziert, dass 60 % der Sicherheitsvorfälle auf Probleme mit Dritten zurückzuführen sein werden. Sicherheitsverantwortliche sind sich des erhöhten Risikos bewusst und arbeiten daran, ihre Sicherheitsvorkehrungen zu verstärken.

Laut der CIO-Umfrage 2021 von Gartner[2] stand Cyber- und Informationssicherheit ganz oben auf der Liste der geplanten Investitionen für 2022, wobei 66 % aller Befragten erwarten, die entsprechenden Investitionen im nächsten Jahr zu erhöhen. Eine andere Umfrage[3] zeigt, dass die Akzeptanz von Endpoint Detection and Response (EDR) voraussichtlich um über 25 % steigen wird. Doch auch wenn Unternehmen mehr investieren, **bleiben sie anfällig** für Kompromisse durch Ransomware, unbekannte Malware-Varianten und Zero-Day-Schwachstellen.

Vorbeugen statt nur Reagieren!
Der „Prävention zuerst"- Ansatz zum Stoppen von Bedrohungen sollte **als Ergängzung** zu bestehende EDR-Lösungen in Betracht gezogen werden, um das Risiko abzumildern. Das Verhindern von Malware vor deren Ausführung und das Verringern von Fehlalarmen verbessert den Betrieb, senkt die Kosten und stoppt bekannte, unbekannte und Zero-Day-Bedrohungen, einschließlich Ransomware, bevor sie die Möglichkeit haben die Umgebung zu infizieren.

Reicht EDR aus, um sich gegen die Bedrohungen von heute und morgen zu schützen?
Die unvermeidliche Wahrheit ist, dass EDR zu spät ist, um Unternehmen von Bedrohungen zu schützen.

Sicherheitsverantwortliche haben ihre Sicherheitssysteme unter der Prämisse aufgebaut, dass Prävention nicht möglich ist. Man war der Meinung, dass Erkennung und Reaktion das beste Mittel gegen den katastrophalen Verlust von Daten und Kundenvertrauen sind.

Die Mentalität des „angenommenen Einbruchs" wurde als der beste Weg nach vorn akzeptiert, und die Idee, dass es nicht darauf ankommt *ob*, sondern wann man kompromittiert wird, ist zur gängigen Weisheit geworden.

1 https://www.darkreading.com/risk/firms-will-struggle-to-secure-extended-attack-surface-in-2022

2 https://www.gartner.com/en/newsroom/press-releases/2021-10-18-gartner-survey-of-over-2000-cios-reveals-the-need-for-enterprises-to-embrace-business-composability-in-2022?subject=

3 https://www.reportlinker.com/p06129743/Endpoint-Detection-and-Response-Market-Growth-Trends-COVID-19-Impact-and-Forecasts.html?utm_source=GNW

SecOps-Teams wurden darauf vorbereitet, bei der Verfolgung von Kompromissindikatoren (IoCs) wachsam zu bleiben und Angreifer aufzuspüren und zu stoppen, die versuchen, sich seitlich zu bewegen, um von innerhalb des Netzwerks aus die Kontrolle zu übernehmen. Maschinelles Lernen (ML) wurde von EDR-Anbietern übernommen, um die Verhaltensanalyse zu automatisieren, Anomalien aufzudecken und Angreifer zu entlarven, bevor sie Schaden anrichten.

Weil sich die kriminellen Akteuren und ihre Methoden weiterentwickelten, gab es weiterhin erfolgreiche Einbrüche.

Die primäre Funktion von EDR ist die Überwachung von Endpunkten, um bösartiges Verhalten nach der Kompromittierung zu erkennen. Es ist eine hervorragende Lösung für die Untersuchung mit forensischen Beweisen, die Suche nach Bedrohungen und die Korrelation von Ereignissen für eine effektive Reaktion und Abhilfe. EDR glänzt, wenn es darum geht, die Absichten eines Angreifers zu ergründen, aber es kann den Angriff nicht von vornherein verhindern.

1. Trügerische Sicherheit durch EDR

Es hat sich gezeigt, dass konstante Sicherheitsschulungen der Mitarbeiter:innen, um sie davor zu warnen, verdächtige Links nicht zu klicken, keine verlässliche Strategie darstellen. Ebenso haben sich automatische Tools, die auf Regeln und Signaturen basieren, als ineffizient gegenüber Malware und Varianten herausgestellt. Die Idee, dass man in der Defensive ist und ständig attackiert wird, hat die Anzahl der Attacken nicht verringert, sondern im Gegenteil, große Verletzungen nehmen zu.

2. EDR ist ein reaktiver Ansatz

Die Wirksamkeit von EDR bei der Abwehr von Angriffen ist begrenzt. Zwar liegt der Fokus von EDR auf der Erkennung von ungewöhnlichem Verhalten, jedoch geschieht dies erst, nachdem der Angriff bereits erfolgt ist. Dies führt zu einem Wettlauf gegen die Zeit, denn bevor die Angreifer die Daten exfiltrieren, verschlüsseln oder das Netzwerk brechen können, müssen sie erkannt werden. Klassisches EDR benötigt oft Minuten, Stunden oder sogar Tage, um ungewöhnliches Verhalten zu identifizieren. Dies erhöht das Risiko, dass böswillige Akteure ihre Spuren verwischen und später aktivieren können

„Nur ein paar Dateien wurden verschlüsselt, bevor wir sie gestoppt haben“, ist eine häufige Aussage von SOC-Teams, die EDR einsetzen. Aber die Frage, die man sich stellen sollte, ist: „Was haben die Angreifer sonst noch getan, bevor sie mit der Verschlüsselung begonnen haben?“

Erst nachdem die Angreifer erfahren haben, dass sie bemerkt wurden, beginnen sie mit der Verschlüsselung. Können Sie sicher sein, dass Sie den Angriff entdeckt haben, bevor er Dropper hinterlassen und/oder Ihre Daten exfiltriert hat? Die Antwort ist in fast allen Fällen ein schallendes „Nein“. Eine proaktive Prävention hingegen stoppt Gefahren, bevor sie das Netzwerk überhaupt kompromittieren können. Indem potenzielle Angriffe im Vorfeld erkannt und blockiert werden, kann die Sicherheit des Netzwerks effektiver gewährleistet werden.

3. EDR verliert im Kampf gegen Ranmsomware

Die Chance auf finanzielle Gewinne und die niedrige Einstiegshürde machen Ransomware und RaaS zu einer ernsthaften Gefahr für fast jede Branche. Dabei setzen die Angreifer auf bekannte, aber auch auf neuartige Malware-Varianten wie Zero-Day-Attacken und Ransomware.

Die Anzahl der Angriffe übersteigt mittlerweile jede Kapazität, um sie rechtzeitig zu stoppen. Die US-amerikanische Finanzbehörde Treasury berichtet, dass allein im Jahr 2021 die durchschnittliche Ransomware-Auszahlung bei über 102,3 Mio USD pro Monat lag1. Doch nicht alle Vorfälle werden gemeldet, um negative Auswirkungen auf Aktienkurse und Kundenbeziehungen zu vermeiden.

> *Wenn EDR ausreichend wäre, würde die Anzahl der erfolgreichen Ransomware-Attacken sinken, und nicht steigen.*
>
> DBConcepts

Die Anzahl der, noch niemals gesehene Malware nimmt alarmierend zu. Mittlerweile sind es

250.000

neue Marware-Varianten pro Tag!

1 https://www.techrepublic.com/article/the-number-of-false-positive-security-alerts-is-staggering-heres-what-you-can-do-to-reduce-yours

4. EDR verursacht eine hohe Anzahl an Fehlalarmen, die das SOC lahmlegen

Der gut dokumentierte Fachkräftemangel in vielen Bereichen der Cybersicherheit hat zu einem intensiven Wettbewerb um qualifizierte Mitarbeiter:innen geführt. Sicherheitsteams müssen effizienter arbeiten, haben aber mit einer großen Anzahl von Alarmen mit geringer Aussagekraft und einer Zunahme von falsch-positiven Alarmen zu kämpfen, was die Teams vor die Herausforderung stellt, das Signal vom Rauschen zu trennen.

In einem großen Unternehmen kann ein EDR täglich Zehntausende von Warnmeldungen generieren, wobei die größten Unternehmen Millionen von Warnmeldungen

verarbeiten. COVID-19 hat das Problem weiter verschärft: Laut Palo Alto Networks haben 47 % der Unternehmen seit dem Beginn der Pandemie mehr Warnmeldungen erhalten. Eine kürzlich durchgeführte ESG-Umfrage ergab, dass 9 von 10 Befragten angeben, dass Fehlalarme ein Problem für ihr Unternehmen darstellen. [1] Laut einer Fastly/ESG-Umfrage[2] verursachten Fehlalarme 46 % der Ausfallzeiten von Anwendungen, und 75 % der Unternehmen verbringen genauso viel oder mehr Zeit mit Fehlalarmen wie mit tatsächlichen Angriffen.

Die Verfolgung von Fehlalarmen hält SOC-Teams davon ab, Aufgaben der Sicherheitshygiene wie das Patchen und Härten von Systemen durchzuführen. Senkung der Anzahl von Alarmen und Fehlalarmen, erhöht die Effektivität des Sicherheitsteams. Das EDR wird Teil der Lösung und nicht Teil des Problems.

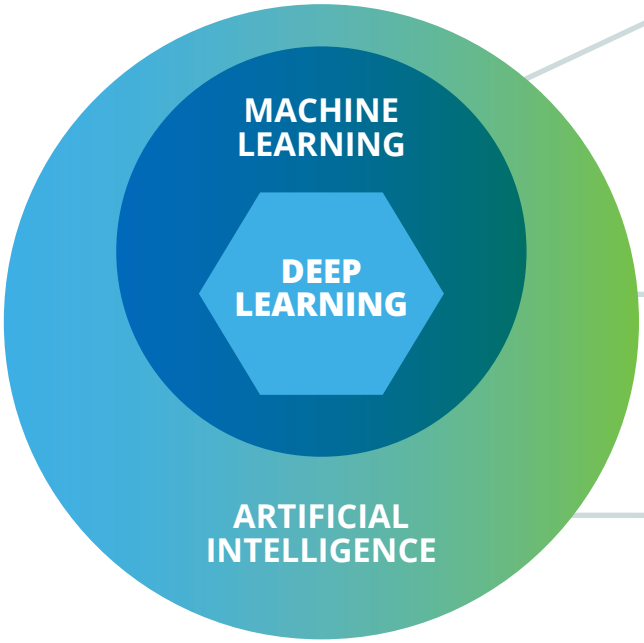
1 https://www.techrepublic.com/article/the-number-of-false-positive-security-alerts-is-staggering-heres-what-you-can-do-to-reduce-yours

2 Reaching the Tipping Point of Web Application and API Security " ESG Researh Insights report –July 2021. // also commissioned by Fastly

5. Machine Learning (ML) schwächt EDR-Effizienz & ML kann ausgenutzt werden

Ungeachtet von EDR wird ML wird von den meisten Sicherheitslösungen übernommen. ML bietet zwar automatisierte Möglichkeiten Verhaltensweisen in Echtzeit zu analysieren, hat aber erhebliche Probleme, wenn es darum geht, Angriffe zu erkennen, bevor die Angreifer Schaden anrichten können.

ML ist immer noch von Menschen abhängig, die die Modelle kontinuierlich trainieren und abstimmen. Wenn eine neue Bedrohung erkannt wird, müssen neue Modelle erstellt und dem Bedrohungsdaten-Feed hinzugefügt werden. Da Menschen anfällig für Verzerrungen und Fehler sind, wissen wir, dass dies auch für ihre Modelle gilt.



MACHINE LEARNING
Teilbereich der KI-Technik, bei dem statistische Methoden eingesetzt werden, um Maschinen zu ermöglichen, sich mit zunehmender Erfahrung zu verbessern.

DEEP LEARNING
Subset von ML, das die Berechnung von mehrschichtigen neuronalen Netzen ermöglicht.

ARTIFICIAL INTELLIGENCE
Eine Technik, die es Maschinen ermöglicht, menschliches Verhalten zu imitieren.

EDR ist auch von der Cloud abhängig, um ML-Erkennungsmodelle und Threat Intelligence Feeds zu prüfen, um Entscheidungen über die Art der stattfindenden Aktivitäten zu treffen, was Angreifern ausreichend Zeit gibt, ihren Angriff auszuführen oder Artefakte zu hinterlassen. Die Abhängigkeit von der Internetverbindung bedeutet, dass EDR keine Bedrohungen erkennen kann, wenn die Systeme ausgefallen sind. Deep Learning hingegen nutzt autonome Prozesse, die der Struktur des menschlichen Gehirns nachempfunden sind, um große Mengen an Rohdaten einzugeben und Informationen vorherzusagen und zu klassifizieren. Dies führt zu einer schnelleren und präziseren Entscheidungsfindung (vor der Ausführung) ohne ständige, vom Menschen abhängige Abstimmung. Ein auf Deep Learning basierender Prevention-First-Ansatz ist nicht von der Cloud abhängig und erfordert keine Internetverbindung, um Entscheidungen in <20 ms zu treffen.

6. EDR ist nur so gut, wie seine Sichtbarkeit innerhalb jedes Endpoints

Die Wirksamkeit Ihrer EDR-Lösung hängt maßgeblich von der Sichtbarkeit Ihrer Endpunkte ab. Eine vollständige Abdeckung aller mit dem Netzwerk verbundenen Endpunkte ist unerlässlich, um umfassenden Schutz und optimale Hygiene zu gewährleisten.

Nur ein winziger Bruchteil der Befragten in der „Voice of SecOps 2021"-Studie von Deep Instinct[1] erklärten, dass sie tatsächlich 100 % ihrer Endpunkte schützen könnten. Zudem gaben nur 35 % der Befragten an, dass alle ihre Endpunkte den gleichen Grad an Transparenz aufweisen und somit ein konsistentes Patching gewährleisten können.

Es zeigt sich auch, dass die Bereitstellung von EDR in hybriden Umgebungen eine große Herausforderung darstellt, wie die Tatsache belegt, dass nur 63 % der Endgeräte mit mindestens einem Sicherheitsagenten ausgestattet waren. Diese Schwachstelle in der Sicherheitskette kann von Angreifern ausgenutzt werden, um in das Netzwerk einzudringen.

Ein alarmierendes Beispiel hierfür ist der SUNBURST-Angriff auf SolarWinds, bei dem Malware zum Einsatz kam, die das Vorhandensein bestimmter EDR-Lösungen aufspüren und ihre Schadfunktion nur dann aktivieren sollte, wenn sie einen ungeschützten Endpunkt gefunden hatte, um so die EDR-Sicherheitskontrollen zu umgehen.

> *Ihre Sicherheit ist nur so gut wie ihr schwächstes Glied – oder besser gesagt, ihr ungeschützter Endpunkt.*
>
> DBConcepts

1 https://info.deepinstinct.com/tof/voice-of-secops-2021

7. EDR blockiert Post-Execution sie verhindert nicht Pre-Execution

Es ist möglich, dass Systeme durch einen blockierten Ransomware-Angriff immer noch verschlüsselt werden können. Das Verhindern eines Ransomware-Angriffs hingegen, schließt diese Möglichkeit aus.

Wenn Sie eine Bedrohung blockieren, stellen Sie sich ihr in den Weg, doch es besteht die Chance, dass sie bereits in Betrieb ist und ihre Spuren hinterlässt. Eine proaktive Verhinderung von Malware und dateilosen Angriffen sorgt dafür, dass die Bedrohung nicht einmal in die Umgebung eindringen kann und bereits im Keim erstickt wird.Die EDR-Erkennung erfolgt in der Regel in den folgenden Schritten:

1. **Warten, bis die Datei gelesen wird.**
2. **Durchführung einer Cloud-Suche nach der Signatur.**
3. **Beobachten Sie das Verhalten.**
4. **„Blockieren“ der Ausführung, wenn EDR ein bösartiges Verhalten entdeckt.**
5. **Nach dem „Blockieren“ des Angriffs muss das Team dann aufräumen und Abhilfe schaffen.**

> *Deep Learning ermöglicht eine Vorbeugung vor der Ausführung und stoppt Bedrohungen mit höchster Genauigkeit, Geschwindigkeit und Skalierung.*
>
> DBConcepts

8. XDR macht EDR weniger effektiv

Angesichts des Hypes um XDR sowie den zahlreichen Versprechungen, könnte man annehmen, dass XDR Ihr EDR wirksamer gestaltet. Tatsächlich ist XDR jedoch auf Erkennung und Reaktion beschränkt und bleibt somit in der Vergangenheit stecken.

Das grundlegende Problem der „zu späten“ Erkennung bleibt nach wie vor bestehen und XDR geht in Bezug auf die Bedrohungslandschaft sowie die Verringerung der Angriffsfläche in die falsche Richtung. Ohne eine grundlegende Lösung, die Warnungen und Fehlalarme reduziert und verhindert, dass unbekannte Angriffe das Netzwerk von vornherein infizieren, wird das Sichten von mehr Telemetriedaten den Angreifern eher mehr Zeit zum Durchführen ihrer Angriffe geben.

Sicherheitslösungen müssen enger integriert werdem, um effektiver zu sein. XDR hat das Potenzial, Telemetriedaten von Sicherheitstools im gesamten Netzwerk sowie in Schlüsselbereichen wie Endpunkten, Cloud und Identität zu zentralisieren. Allerdings besteht die Sorge, dass die alleinige Zunahme der Daten die Suche nach der Nadel im Heuhaufen erschwert und letztendlich die Betriebskosten erhöht sowie Entscheidungen verzögert.

FAZIT

- **EDR reicht einfach nicht aus, um die komplexen Bedrohungen von heute zu verhindern, geschweige denn die Angriffe von morgen.**
- **Die Zukunft der Cybersicherheit ist auf Deep Learning-basierte Prävention**

Wir empfehlen Deep Instinct: Mit dem weltweit ersten und einzigen speziell entwickelten Deep-Learning-Framework für Cybersicherheit setzt Deep Instinct voll auf Prävention, um Ransomware und andere Malware zu stoppen. Damit werden unbekannte Bedrohungen schneller und effektiver als jede andere EPP- und EDR-Lösung verhindert und sichergestellt, dass Malware niemals in der Umgebung ausgeführt wird.

- **<99 % der bekannten und unbekannten Zero-Day-Gefahren stoppen**
- **Gefahren in unter <20 MS verhindern**
- **Falsch-Positive Meldunngen auf <0,1% reduzieren.**

Haftungsausschluss

Dieses Dokument dient ausschließlich zu Informationszwecken. Die Inhalte wurden von Deep Instinct zur Verfügung gestellt. (Mit freundlicher Genehmigung von Deep Instinct). Alle Informationen wurden nach bestem Wissen und Gewissen erstellt. DBConcepts übernimmt keinerlei Gewähr für die die Richtigkeit, Aktualität, Korrektheit, Vollständigkeit oder Qualität der bereitgestellten Informationen.

Haftungsansprüche gegen DBConcepts, welche sich auf Schäden materieller oder ideeller Art beziehen, die durch die Nutzung oder Nichtnutzung der dargebotenen Informationen bzw. durch die Nutzung fehlerhafter und unvollständiger Informationen verursacht wurden, sind grundsätzlich ausgeschlossen, sofern seitens des Autors/DBConcepts kein nachweislich vorsätzliches oder grob fahr-
lässiges Verschulden vorliegt.

DBConcepts behält es sich ausdrücklich vor, Teile dieser Informationen oder das gesamte Dokument ohne gesonderte Ankündigung zu verändern, zu ergänzen, zu löschen oder die Veröffentlichung zeitweise oder endgültig einzustellen.

DBCONCEPTS

DBConcepts GmbH • Ares Tower
Donau-City Straße 11 • 1220 Wien
Tel.: +43 1 890 89 99-0
office@dbconcepts.com

DBConcepts Deutschland GmbH
Kleestr. 21-23 • 90461 Nürnberg
Tel.: +49 911 969595 00
office@dbconcepts.com